

TECH SUPPORT SCAMS

You get a phone call, pop-up, or email telling you there's a problem with your computer.

Often, scammers are behind these calls, pop-up messages, and emails. They want to get your money, personal information, or access to your files. This can harm your network, put your data at risk, and damage your business.

HOW THE SCAM WORKS

The scammers may pretend to be from a well-known tech company, such as Microsoft. They use lots of technical terms to convince you that the problems with your computer are real. They may ask you to open some files or run a scan on your computer — and then tell you those files or the scan results show a problem...but there isn't one.

The scammers may then:



Ask you to give them remote access to your computer — which lets them access all information stored on it, and on any network connected to it



Install malware that gives them access to your computer and sensitive data, like user names and passwords



Try to sell you software or repair services that are worthless or available elsewhere for free



Try to enroll you in a worthless computer maintenance or warranty program



Ask for credit card information so they can bill you for phony services or services available elsewhere for free



Direct you to websites and ask you to enter credit card, bank account, and other personal information